ABSTRACT

A method and apparatus for generating encryption stream ciphers. The recurrence relation is designed to operate over finite fields larger than GF(2) and is maximal length. An output equation generates the output based on a plurality of elements in the shift register used to implement the recurrence relation. The recurrence relation and the output equation are selected to have distinct pair distances such that, as the shift register shifts, no particular pair of elements of the shift register are used twice in either the recurrence relation or the output equation.